Submitted
Paul

Paper to be presented at the Pacific Basin Nuclear Conference (PBNC98)
May 1998
Banff, Alberta, Canada

SEVERE CORE DAMAGE FREQUENCY AND INSIGHTS FROM CANDU® 6 LEVEL 1 PROBABILISTIC SAFETY ASSESSMENT

P.A. Santamaura[1], J. G. Tielemans[2], T.H. Nguyen[1], . H.S. Shapiro[1], R.E.B. Henderson[1], and B.A. duQuesnay[1]

1. Atomic Energy of Canada Limited
2251 Speakman Drive
Mississauga, Ontario, CANADA L5K 1B2

2. Spectrum Consulting Inc.
544 McDonnel Street
Peterborough, Ontario, CANADA K9J 6Z8

Applications of Probabilistic Safety Assessments to Plant Operation

submitting author/speaker:
Paul A. Santamaura
Atomic Energy of Canada Limited
2251 Speakman Drive
Mississauga, Ontario, CANADA L5K 1B2
Tel: (905) 823-9060 Ext 5032
Fax: (905) 823-9631
e-mail: santamaurap@aecl.ca

key words: Level 1 PSA, PSA internal events, core damage

SEVERE CORE DAMAGE FREQUENCY AND INSIGHTS FROM CANDU® 6 LEVEL 1 PROBABILISTIC SAFETY ASSESSMENT

P.A. Santamaura[1], J. G. Tielemans[2], T.H. Nguyen[1], . H.S. Shapiro[1], R.E.B. Henderson[1], and B.A. duQuesnay[1]

1. Atomic Energy of Canada Limited
2251 Speakman Drive
Mississauga, Ontario, CANADA L5K 1B2

2. Spectrum Consulting Inc.
544 McDonnel Street
Peterborough, Ontario, CANADA K9J 6Z8

ABSTRACT

An internal events Level 1 probabilistic safety assessment (PSA) of a CANDU® 6 nuclear power plant (NPP) was conducted by AECL and KAERI, with Wolsong NPP 2/3/4 in Korea taken as the reference plant. Wolsong NPP 2/3/4 is an enhanced design of Wolsong NPP Unit 1, which has been operating successfully since 1983. The reference plant has a number of safety and design improvements compared to Wolsong NPP 1. Based on the PSA, the summed severe core damage frequency for Wolsong NPP 2/3/4 is estimated to be 6.1E-6 events per year for internal events. Initiating events that dominate the severe core damage frequency are loss of class IV electrical power, dual digital computer control failure, loss of end shield cooling and loss of service water. They contribute 24%, 17%, 16% and 12% respectively to the summed severe core damage frequency. The results of this PSA confirm a low severe core damage frequency.

1. INTRODUCTION

The CANDU® 6 Pressurized Heavy Water Reactor (PHWR, 600-700 MWe net range) is the major commercial CANDU (CANada Deuterium Uranium) nuclear reactor, with plants presently operating or under construction in Canada, Korea, Argentina, Romania and China. In order to ensure a high degree of safety and reliability, the safety design philosophy of the CANDU reactor is based on the concepts of separation, independence, redundancy, and diversity in the equipment, cabling and piping of safety systems. Testability of the equipment is crucial to meeting reliability requirements.

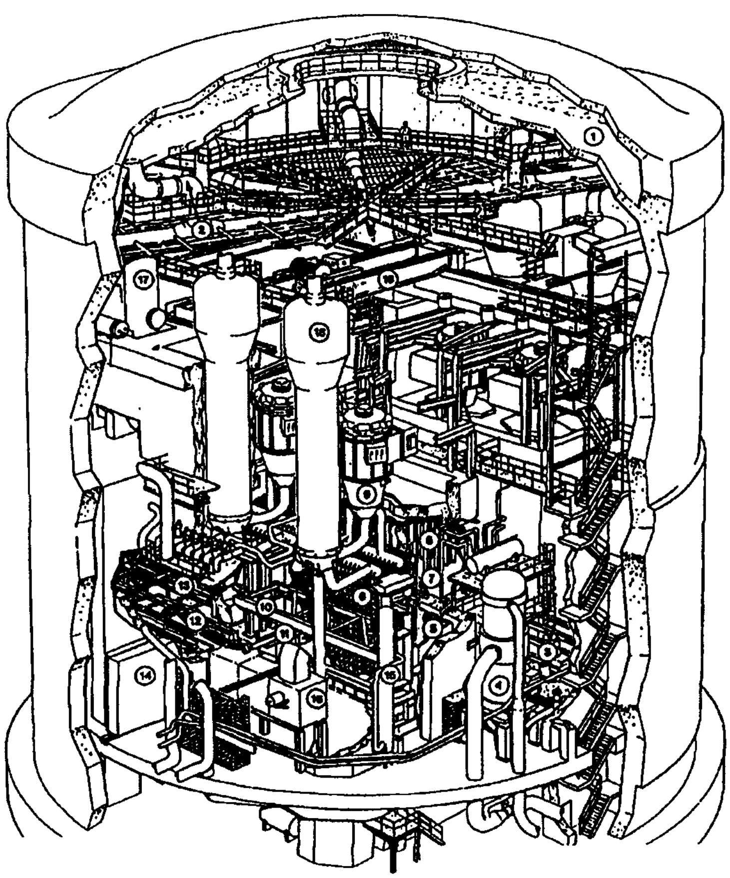
The CANDU 6 reactor was originally designed in the mid-seventies as a single unit plant. It has consistently produced one of the best operating records for performance (Howles, 1995). The CANDU 6 incorporates design features which limit the progression of a severe accident sequence:

1) Two redundant and diverse reactor shutdown systems which lead to a very low probability of a reactivity induced accidents and anticipated transient without scram. High pressure melt ejection is excluded by design.
2) Pressure tube design which separates the high-pressure, high-temperature primary coolant from the low-pressure, low-temperature moderator fluid. This design creates an additional heat sink, and requires that in addition to loss of internal cooling, the moderator also has to be lost for a severe core damage to occur.

3) Achieving recriticality of CANDU bundles in ordinary (light) water is not possible because of the use of natural uranium. Natural uranium fuel requires a heavy water moderator to achieve and sustain criticality.
4) The shield tank and end shields which surround the moderator contain light water for biological and thermal shielding and provide additional back up heat sinks. If core damage occurs, the shield tank can absorb decay heat from any debris in the calandria vessel and contain the debris as long as shield tank water inventory is available, thus delaying further progression of a severe accident. Over 5000Mg of water in the shield tank must boil off before any core-concrete interactions may occur.

As a single unit plant design, the CANDU 6 has proven to be safe and reliable. The Wolsong NPP has taken this reliable design as the foundation for its multi-unit plant. The strengths of this design, coupled with the sharing of some services between pairs of reactors has resulted in an economical solution for Korea's power generation requirements.

The main nuclear steam supply system components for a CANDU 6 reactor are shown in Figure 1.



1 Dousing Tank Water
2 Dousing tank Valves
3 Moderator Pump
4 Moderator heat Exchangers
5 Feeder Cabinets
6 Reactor Face
7 Reactor
8 Reactivity Mechanisms
9 Primary Heat Transport System Pump
10 Fuelling Machine Bridge
11 Fuelling Machine carriage
12 Fuelling machine Catenary
13 Fuelling Machine Maintenance Lock
14 Fuelling Machine Maintenance Lock Door
15 End Shield Colling Water Delay tank
16 Vault Cooler
17 Pressurizer
18 Steam Generator
19 Steam Generator Room Crane

Figure 1
CANDU 6 Main Nuclear Steam Supply Components in Reactor Building

Reliability assessments have been used in CANDU designs since the early 1960s. From 1975 to 1983, a number of probabilistic assessments using safety design matrices (SDM) were conducted. In 1995, a comprehensive Wolsong NPP 2/3/4 Level 1 PSA for internal events was completed by AECL.

The Wolsong NPP 2/3/4 PSA was developed in two phases:

1) Phase I - PSA analysis is to confirm that the design is acceptable based on conservative CANDU ground rules (Santamaura et al, 1995). The objectives of this phase were:
   - i) to demonstrate that Canadian regulatory requirements were met, including special safety systems reliability requirements;
   - iii) to identify any weaknesses in the design;
   - iv) to provide input into operational and abnormal operating manuals;
   - v) to support the application for the operating license for Wolsong NPP 2/3/4.

The acceptance criteria was based on a design target frequency of 1E-6 events/year or less for individual beyond-design-basis accident sequences. This work was conducted jointly by AECL and KAERI, the Korea Atomic Energy Research Institute. The composition of the PSA team consisted of 60% Korean and 40% Canadian personnel. The success of the PSA demonstrates the benefits of international cooperation. The objectives were met for this phase. Since recovery analysis was applied only to sequences with frequencies above 1E-6/y, the results were conservative.

2) Phase II - The objective of the second phase is to reduce some and eliminate other conservatisms from Phase I and then to calculate a summed severe core damage frequency. As is typically done for US LWRs, a 24 hour mission time is used. The basis of this value is a combination of engineering judgement and the assumption that the operator can take recovery actions to stabilize the situation after 24 hours. Obviously for some accidents, cooling capability and containment isolation of the reactor must be maintained longer than 24 hours. Canadian practice has been to model some mitigating systems, such as, emergency core cooling for at least a 1-month mission time.

The severe core damage results and insights from the Phase II Level 1 PSA for internal events for Wolsong NPP 2/3/4 are described in the following sections. This analysis does not include fire and seismic events.

2. METHODOLOGY

The Phase II PSA uses the same methodology as the Phase I PSA analysis (Santamaura et al, 1995), with the exception of more extensive recovery analysis for individual accident sequences.

The methodology of the Wolsong 2/3/4 PSA involved developing medium event trees with post-accident operator actions modelled in the event trees. In addition, detailed system fault trees were developed. Initiating events for full power operation events having similar characteristics and anticipated plant responses were grouped, resulting in 47 events that required detailed analysis. Initiating event frequencies were determined by fault tree analysis, and in some cases, from operating experience. Over 400 accident sequences were quantified.

A generic CANDU reliability database was used for calculation of frequencies and probabilities of component failures. Systems were modelled to the component level, including process, control and instrumentation equipment. Systems modelling included running and starting failure rates and test intervals. Parametric common cause failure analysis was not considered. Fault trees for twenty-five mitigating systems were developed. Merging the support systems with front line systems resulted in fault trees with over 1900 intermediate gates and 2600 basic events for some systems. Sensitivity, uncertainty, and importance analyses were performed using Science Applications International Company (SAIC) CAFTA evaluation software (Koren et al, 1987). In addition, a number of programs were developed in-house to assist in the accident sequence quantification and recovery analysis.

The following conservatisms were reduced or eliminated to obtain a best estimate summed core damage frequency for Phase II:

1) Crediting the emergency core cooling system (ECC) and moderator systems for decay heat removal in loss of heat removal sequences at high heat transport pressure (transient events),
2) Performing recovery analysis on all cutsets with a frequency greater than 1E-9 events/year,
3) Reduction of mission time for emergency core cooling and moderator acting as a heat sink from 3 months to 24 hours,
4) Crediting the moderator as a heat sink for sequences with dual digital computer control failure and consequential LOCA, occurring at low heat transport pressure with ECC failure,
5) Grouping of multiple initiating events which have not occurred, but which have the same or similar plant response(s), such as small LOCAs,
6) Dividing loss of end shield cooling initiating events into loss of flow and loss of heat sink based on results from the PSA support analysis,
7) Updating the fault tree logic based on recent design information.

The Phase I PSA used a relatively simple screening model since operating procedures and instructions were not available. It was based on available operator action time and included diagnosis errors only. As well, a second operator action on a failed action was not credited in the event trees. The same human reliability analysis (HRA) model was retained in the Phase II analysis.

Eleven categories of plant damage states (PDS) were identified in the analysis. Three PDS cover beyond design basis accidents (PDS0, PDS1 and PDS2) that include events leading to loss of the core structural integrity or multiple failure of fuel channels.

3. SEVERE CORE DAMAGE ACCIDENTS

In a CANDU reactor, not all severe accidents may result in a severe core damage. In addition, the severe core damage may occur only at low pressures. Consider the traditional definition of a severe accident - loss of primary coolant with a failure to makeup the coolant with emergency core coolant injection. For CANDUs such events are analyzed as part of the design basis accidents and it has been demonstrated by many analyses and experiments that the moderator acts as an effective heat sink for hot, voided channels and helps maintain channel integrity. While fuel damage is not precluded for these accidents and local deformations in pressure tubes may also occur, the integrity of all channels is maintained and no ejection of hot melt can be envisioned. For these accidents to progress to a severe core damage the moderator must also be lost. Once the moderator is lost, the core integrity is lost by disassembly by heatup of hot, depressurized channel segments. Thus a severe core damage accident is one that involves a loss of moderator coolant after a sustained loss of primary coolant.

With redundant shutdown systems, reactivity induced accidents are screened out as being of extremely low probability. Probabilistic analyses show that a majority of the severe accidents do not start out as LOCAs, but as transients involving an initial or consequential loss of main feedwater and a loss of other heat sinks such as the auxiliary feedwater, the shutdown cooling system, and the emergency water supply (EWS). For a large fraction of these accidents, following the steam generators dryout, the water level in the calandria falls to expose high power upper elevation channels. The heatup of a lead channel at high pressures leads to its rupture into the moderator. Once the first channel fails, the heat transport system is expected to depressurize relatively fast (in seconds) and induce the injection of the high pressure ECC from the accumulators. This results in arresting any further core damage. Therefore scenarios with available ECC do not lead to severe core damage and are not counted as such. For these scenarios, long term cooling is maintained by ECC heat exchangers and/or by moderator heat exchangers. Severe core damage invariably starts under depressurized conditions upon loss of the moderator heat sink to hot channels it envelops. Thus the three distinguishing features of severe core damage in CANDU reactors are : no early damage, no damage at high pressures and no damage for cases where the ECC is available.

4. RESULTS

The CANDU 6 summed severe core damage frequency (SCDF) has been estimated at 6.1E-6 events per year for internal events. Initiating events that dominate the severe core damage frequency are loss of class IV electrical power, dual digital computer control failure, loss of end shield cooling and loss of service water. As shown in Figure 2, these initiating events represent 24%, 17%, 16% and 12%, respectively, of the summed severe core damage frequency.

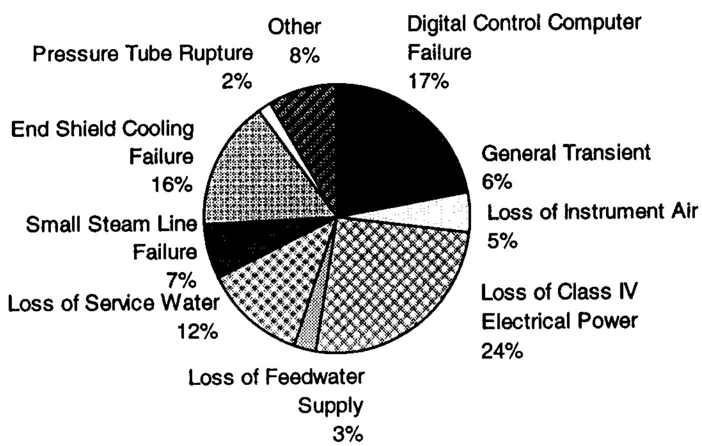


Figure 2
Summed severe core damage frequency

The top 5 severe core damage sequences are listed in Table 1. The highest SCDF is from a postulated loss of class IV electrical power as an initiating event with multiple mitigating system failures and is estimated at 6.9E-7/y. The mitigating systems that must all fail to induce a severe core damage include a loss of auxiliary feedwater system, a loss of shutdown cooling system, as well as a loss of emergency water supply system and a loss of ECC (dormant failure). In addition, the operator must fail to take recovery actions.

The summation of severe core damage sequences with a post-accident operator failure is 4E-6/y. Since this is a significant portion of the total, it implies that the SCDF is highly sensitive to the post-accident operator model. The results also show the significance of transient events leading to severe core damage.

The SCDF result is similar to those previous published CANDU summed core damage frequencies which showed a SCDF of 6.2E-6/y (Shapiro, Smith, 1986). Although the results are similar, the methods and assumptions were different. The present study includes control and instrumentation modelling, incorporation of testing and human error in maintenance in the fault trees, as well as mission unreliability. The present study also includes ECC credit on transient events and detailed recovery analysis which reduces the SCDF value significantly. The results show that, for internal events, the summed severe core damage frequency is acceptably low.

Table 1

Top Five Severe Core Damage Sequences for 24–hour Mission Time

Plant Damage State	Severe Core Damage Frequency (y^{-1})	Sequence Name	Description of Sequence Events listed are system failures unless preceded by a "/"
PDS1	6.9E-07	CL4-R13D	IE-CL4*R60E4*AFW*SDC-ABN*EWS1*ECC-D*/RS*/CLPRV*/SGPR*/OSDC2B*/OEWS1B
PDS1	5.5E-07	CL4-R14D	IE-CL4*R60E4*AFW*SDC-ABN*OEWS1B*ECC-D*/RS*/CLPRV*/SGPR*/OSDC2B
PDS1	4.9E-07	LOSW-R7	IE-LOSW*FW*EWS1*/RS*/CLPS*/PTHT*/OEWS2
PDS1	4.5E-07	ESCF-R4	IE-ESCF*OCC1*/ORSB*/RSHW1*/FW
PDS1	4.2E-07	ESCB-R4	IE-ESCB*OCC*/RRS-SETB*/FW

Other PSA studies for CANDU reactors show similarly low severe core damage frequency predictions. The Darlington Probabilistic Safety Evaluation (Raina et al., 1989) estimated a SCDF of 3.8E-6/y. Although both Darlington and Wolsong use CANDU reactors, there are some significant differences in systems such as the shield tank, containment, standby electrical power, and inter-unit ties for support systems. There are also differences between the PSA methodologies used by Ontario Hydro and AECL. Yet both studies point to low risk from internal events for CANDU reactors.

5. IMPORTANCE MEASURES

The importance measure of a component or system is a measure of its impact on the top event frequency. There are 3 measures of importance generally used in PSA: the Fussell-Vesely (FV) importance, Risk Reduction Worth (RRW) and Risk Achievement Worth (RAW).

The FV importance determines the contribution associated with the individual event or system to the total severe core damage and is expressed as the ratio of the sum of all cutsets containing a specific event to the sum of all cutsets. Figure 3 shows the FV importance values by system. Class III electrical power, EWS and service water are the systems which have the highest FV importance. This is consistent with expectations as Class III electrical power and service water are vital support systems and EWS is required for both LOCA and transient events.

The RRW determines the reduction of risk if the unavailability of a component or system (A) is set to zero (i.e. it does not fail). It is the ratio of the sum of all cutsets to the sum of all cutsets given A=0. Figure 4 shows the RRW by system. As with the FV importance, Class III electrical power is the system which has the highest RRW. This would indicate that improving the reliability of class III electrical power system would provide the greatest improvement in SCDF.

The RAW determines the increase of risk due to a component or system being unavailable (i.e. failed). It is the ratio of the sum of all cutsets given A=1 to the sum of all cutsets. The service water is the system which has the highest RAW. This shows the service water being unavailable contributes the highest risk to the plant.

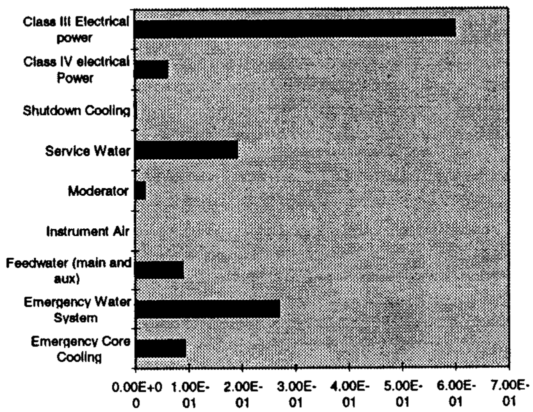


Figure 3

Fussell-Vesely Importance

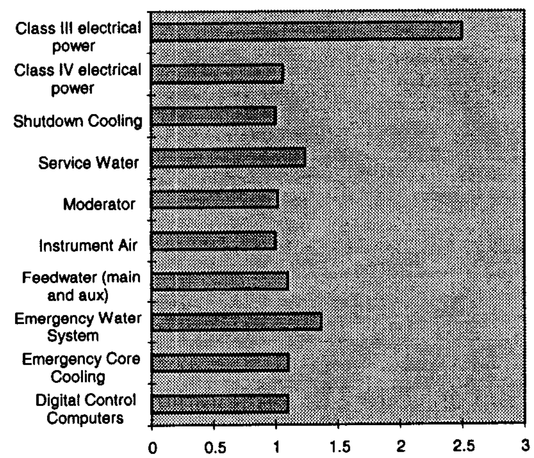


Figure 4
Risk Reduction Worth

6. SENSITIVITY ANALYSIS

An analysis was also performed to test the sensitivity of the results to variabilities in modelling parameters such as failure rates, mission times, and human errors. Table 2 lists some results of the sensitivity analysis.

Table 2
Sensitivity Analysis Results for 24-Hour Mission Time

Sensitivity Variable	Basic Event Multiplication Factor	New Severe Core Damage Frequency	Ratio (New / Original)
Class III standby diesel generators (5211SG1/2--+GD3EFR/EFS)	0.5	4.04E-06	0.66
Valve 3461-PV7 in EWS system (3461PV7--$VGCCFC)	0.1	5.24E-06	0.86
Switchyard restored in 60 minutes (R60E4)	0.2	4.86E-06	0.79
ALL post-initiating event operator actions in event trees	0.5	3.99E-06	0.65
ALL post-initiating event operator actions in event trees	2.0	1.04E-05	1.70
Dual Computer Control Failure (IE-DCC)	0.33	5.40E-06	0.88

These results show the importance of the class III electrical power standby diesel generators and the recovery of class IV electrical power. The probability of failure of diesel generators is based on generic data which has not been updated. The use of CANDU 6 based data has only now become possible since four CANDU 6 reactors have been operating for nearly 15 years.

Preliminary analysis shows that the original generic data is conservative. The SCDF would be lower if the CANDU 6 based diesel failure data are used. The summed severe core damage frequency decreases by 34% when the Class III standby diesel generator failure rate is decreased by 50%. A more detailed human reliability analysis model may also reduce conservatism in the present screening HRA model. This may now be undertaken given that Emergency Operating Procedures have recently been developed. Reducing the probability of errors in post-accident operator actions by 50% reduces the SCDF by 35% to 4E-6/y. By reducing the probability of recovery actions necessary for restoring Class IV electrical power by a factor of 5, the SCDF is reduced by 33%. The sensitivity analysis thus shows that the PSA should be treated as an on-going activity as more data and operating experience is accumulated.

The sensitivity analysis was also performed for 1 month and 3 months mission times and the results are shown in Table 3. The mission time applies to the ECC and moderator systems only (mission time for other systems remained at 24 hours). The SCDF estimates for a 1 month and 3 month mission time increases to 7.7E-6/y and 1.4E-5/y respectively. However, only a limited recovery analysis was conducted for these mission times.

Table 3

Effect of Mission Times on Severe Core Damage Frequency

Mission Time of ECC and Moderator Systems	Severe Core Damage Frequency (events per year)	Remarks
24 hours	6.1E-6	
1 month	7.7E-6	Limited recovery analysis
3 months	1.4E-5	Limited recovery analysis

The sensitivity analysis also shows the significance of ECC mission time on severe core damage frequency.

The results of these analyses serve as important feedback to various design and operating activities (e.g. maintenance planning and design next generation CANDU nuclear power plants).

7. CONCLUSIONS

The summed severe core damage frequency for Wolsong NPP 2/3/4 is estimated at 6.1E-6 events per year for internal events. Initiating events that dominate the severe core damage frequency are loss of class IV electrical power, dual digital computer control failure, loss of end shield cooling and loss of service water. They contribute 24%, 17%, 16% and 12% respectively to the summed severe core damage frequency.

The results indicate the significance of transient events leading to severe core damage. The sensitivity analysis shows the significance of ECC mission time on severe core damage frequency. It confirms that, from internal events, the severe core damage frequency is acceptably low. The importance measures analysis show the significant effect of the unavailability of the service water system.

Three areas of further analysis are 1) the derivation of CANDU 6 specific reliability of diesel generators, 2) the replacement of the screening HRA model with a more detailed one based on Emergency Operating Procedures and 3) the determination of the effect of common cause failures.

ABBREVIATIONS

AFW	Auxiliary Feedwater	OEWS	Operator initiated EWS
CL4	Class IV Power	ORSB	Operator initiates Reactor Shutdown
CLPRV	Consequential LOCA D2O Storage Tank	OSDC2B	Operator initiates Shut Down Cooling (variation)
CLPS	Consequential LOCA via Pump Seals		
ECC-D	Emergency Core Cooling - Dormant		
ESCB	End Shield Cooling - pipe Break	R60E4	Operator Restores Class IV electrical power within 60 minutes
ESCF	End Shield Cooling - loss of Flow	RRS- SETB	Reactor Regulating System - Setback
EWS1	Emergency Water System (Dousing tank only available)	RS	Reactor Shutdown
FW	Feed Water	RSHW1	Reactor Shutdown - Hardware
IE-	Initiating Event (prefix)	SDC	Shut Down Cooling
LOSW	Loss of Service Water	SDC-ABN	Shut Down Cooling - Abnormal
OCC	Operator initiates Crash Cool	SGPR	Steam Generator Pressure Relief
PTHT	PHT Pump Trip - High bearing Temperature		

REFERENCES

Howles, L. "Load Factors to end of September 1994", Nuclear Engineering International, Volume 40, No. 486, pp. 40-44, January, 1995.

Santamaura, P.A. duQuesnay, B.A. Shapiro, H.S. and Yang, J-E, "Overview of the CANDU® 6 Wolsong NPP 2/3/4 Probabilistic Safety Assessment", Proceedings of the International Conference on Probabilistic Safety Assessment Methodology and Applications, PSA'95, Seoul, Korea, November 26-30, 1995, Volume 1, pp.495-500, Korea Atomic Energy Research Institute, Taejon Korea, 1995.

Koren, J. M. and Gaertner, J. "CAFTA: A Fault Tree Analysis Tool Designated for PSA", International Topical Conference on Probabilistic Safety Assessment and Risk Management, PSA '87, Zurich, Switzerland, August 30-September 4, 1987, Volume II, pp.588-592, European Nuclear Society, Zurich, 1987.

Shapiro H. and Smith, J.E. , "Probabilistic Safety Assessments in Canada", Summer National Meeting of the American Institute of Chemical Engineers', Boston, August 1986.

Raina V.M., Webster P.A., Chan E.M., Darlington Probabilistic Safety Evaluation: Review of Results, and Future Applications, Proceedings of the International Topical Meeting on Probability, Reliability and Safety Assessment PSA'89, Pittsburgh, Pennsylvania, USA,
April 2-7, 1987, Volume 2, pp779-786, American Nuclear Society, La Grange Illinois, USA, 1989.